SSRG International Journal of Electrical and Electronics Engineering
ISSN: 2348-8379/ https://doi.org/10.14445/23488379/IJEEE-V10I4P111

Volume 10 Issue 4, 115-122, April 2023
© 2023 Seventh Sense Research Group®

Original Article

Safe, Secure and Efficient Integration of Critical Wireless Sensor Networks for Industrial Applications

Vineeta Philip[1], Pramod Sharma[2], H. B. Magar[3], A. S. Ubale[4], S. O. Ahire[5]

[1, 3, 4, 5]*University of Technology, Jaipur & Faculty of AISSMS Institute of Information Technology, Pune*
[2]*University of Technology, Jaipur*

[1]*Corresponding Author : vineeta.philip@aissmsioit.org*

Received: 02 March 2023 Revised: 31 March 2023 Accepted: 17 April 2023 Published: 29 April 2023

Abstract - *Flexible, mobile, and low-cost wireless communication is gaining popularity in industrial automation. Aside from cryptographic key management, wireless systems generally need extra engineering and maintenance duties. In order for wireless systems to be properly implemented and maintained in the industry, this issue must be solved. In this article, we cover safety and security in a comprehensive manner, regardless of the medium used. By adopting the black channel idea, our proposed system introduces security modules that may enable scratch-to-end Authenticity and integration. Using current autonomously operated gadgets and standard operating procedures like Wireless HART, Profisafe and Profinet IO, We may expand and offer start-to-end functional protection and security by implementing the suggested technique. With periodic and predictable downlink broadcasts, we increase the performance of functional safety protocols as well as the Wireless HART standard.*

Keywords - *Efficient integration, Industrial applications, Safety, Security, WSN.*

1. Introduction

Wireless sensor network (WSN) is broadly considered one of the most significant advances of the twenty-first century [1]. In the previous decades, it has gotten colossal consideration from both the scholarly world and industry everywhere worldwide.

A WSN commonly comprises countless low-cost, low-power, and multifunctional wireless sensor nodes with detecting, wireless correspondences, and calculation capacities [2,3]. These sensor nodes impart over short separations through a wireless medium and work together to achieve a typical errand, for instance, condition observing, military reconnaissance, and modern procedure control [4]. The fundamental way of thinking behind WSNs is that while every individual sensor node's ability is restricted, the whole network's total intensity is adequate for the necessary strategy.

An increasing number of companies are looking at wireless technology to boost flexibility, scalability and efficiency while lowering costs. A lack of device compatibility has impeded implementation rates due to worries about dependability, security, and integration. As a result of these problems, WirelessHART [5] was certified and launched in 2007. Standards like ISA 100.11a are becoming commonplace [6].

These systems use ZigBee [7] or proprietary solutions [8] to read automated metres. Despite the obvious advantages of wireless communications, some traditional fieldbuses will persist. So these two technologies must be smoothly integrated. Wireless communication must be integrated with current fieldbuses or new field networks effectively and securely before it can be utilized and deployed efficiently. This would allow effective communication in regions where cable connectivity is prohibitively expensive, immobile, or mechanically worn out. No perfect answer to efficient integration has been found in most studies on wireless fieldbus extension. A full architecture for secure wireless/wired communication is proposed in this article. Moreover, we demonstrate a novel resolution: periodicity with forecasted communication to actuators from the gateway pertaining to networks of Wireless HART.

2. Literature Review

The networked connections between sensors/actuators and controllers have revolutionized industrial communication in the previous decade. Profibus and Profinet [10] have been addressed in the cabled communication of fieldbus concerning integration, functional safety and security purposes. A full study of automation security is presented in [11]. This is a fantastic place to start. They also offer two ways for tight Profibus/Interbus integration utilizing Profinet IO.

This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

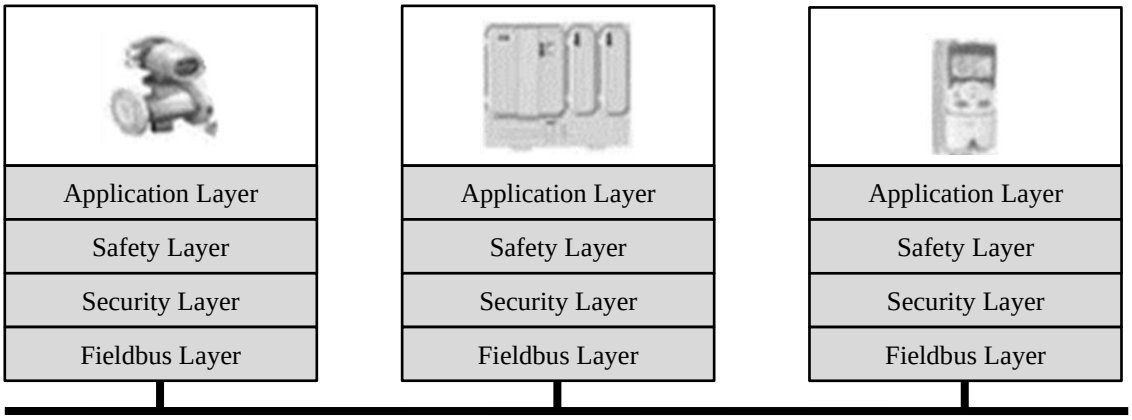

Fig. 1 Proposed methodology for safety and secure communication in iIndustrial WSN

Various wireless automation networks and field bus extensions have been investigated. Willig et al. discuss wireless fieldBus challenges and solutions [12]. Gungor and Hancke present a review of industrial wireless sensor networks in [13]. An experimental assessment employing an industrial application layer protocol for wireless networks is presented in [15]. On many backbone routers, Ishii shows results in 12. To improve wireless industrial automation system dependability. On the other hand, Miorandi and Vitturi [16] looked at the feasibility of using Profibus DP on Ethernet and Bluetooth hybrid networks. On the use of simulation tools in validating Wireless Profibus extensions, Sousa and Ferreira described this in [17]. Research on wireless ProfiBus extensions is documented in [18]. It has recently gained popularity in academics and industrial automation. According to their study [20], WirelessHART and ZigBee technologies function differently. With the standards of WirelessHART, Security remains non-compulsory. However, this is required for ZigBee. For example, Raza et al. showcased an analysis for security pertaining to protocols of WirelessHART to counter known attacks though [21].

In process automation, WirelessHART has been studied for control [22]. Nixon et al. [24] proposed a wireless mesh network to suit the control performance needs (e.g., WirelessHART). They concluded that device and network functioning must be coordinated. It is addressed in IEC 62280-2 [25] for communication and operational protections within open transmission systems and Deuter et al. [26] for Virtual Automation Networks. For Wireless HART integration, Trikaliotis and Gnad compare several mapping systems. Their work has not addressed engineering efficiency, Wireless HART-specific operating procedures, or safety and security-critical intercommunication needs. Wireless Cooperation Team Profibus Internationale is currently working on standardizing Wireless HART devices in Profibus/Profinet networks. Mainly, we employ a comprehensive strategy that includes safety and security, which are not yet standardized. Summarizing our contributions to this study.

- Structure pertaining to wireless and cabled communications that address entire operating security and functional safety. A functional safety framework depending on the black channel [27] idea.
- It is shown utilizing WirelessHART, Profisafe, and Profinet IO, over control systems of industrial applications. By integrating with the WirelessHART network, safety and security settings may get designed. That past work did not include security, or safety is unique.
- WirelessHART actuators may now provide periodic and predictable data to gateways using a novel facility known as the transmission for periodic downlink. A cable-less actuator or one with a temporal limitation may be used with this service.

3. Proposed Methodology

Most protocols for field bus includes safety procedure for wired fieldbus communication. Because of the nature of Open media's nature, most wireless technologies have a security solution. While technology-dependent security measures and capabilities range of non-compulsive (ZigBee) in elaborating besides required (Wireless HART). Together wireless and cabled field-bus systems cause significant issues, notably in terms of integrationand maintenance.

An absence of protection steps in cabled portions and none within cable less part is also shown in Figure 1. Maintenance efficiency and increased design and engineering can be achieved by "seamless Integration". Because it becomes complicated to meet entire criteria for industries having a single protocol/standard.

Several technologies will most likely be used in the future in industrial environments. For this reason, we provide a framework for dealing with heterogeneous network security and safety, which conceals technological variance and gives an integrated scheme.

Our approach is built on the notion of the Black channel, whichaddresses concerns of security and safety irrespective of the kind of media (wired or wireless). As a result, current protocols of transmission and automation gadgets may be reused. The structure covers wired Fieldbus, DCS, PLC, sensor, and actuator, also having wireless networks within an automation system. On the communication layer, amongst the application layer and communication, a layer of a security layer is appended, as shown in Figure 1.

Channel. In abstaining encounters amongst protocols, thereby allowing scratch-to-end security, layers of security were infused amongst the OSI model and the application rather than within the OSI model. Layers of securities were then used between a communication layer and a security layer. Layers of security are part of the black channel for certification purposes. These layers may be used independently of one another, depending on the situation. Scratch-to-end safety and security are achieved by not embedding some additional securities needed for the communication channel.

Moreover, our approach works well with both modular and small-field equipment. Backplane buses and point-of-device accesses are used like black channels to deploy safety/security layers inside a modular device. In a modular I/O system, independent of the security/safety layer, secure, safe with conventional I/O prototypes may be present. As a result of our methodology, safety/ security-enabled devices may coexist alongside current field equipment in various applications. Our solution allows for independent usage of the safety and security layers. Node-to-node deployment of the safety and/or security layer is also possible.

The black channel provides a lot of functionality, so additional redundancy in some layers is added through our approach. Due to the fact that the top levels do not depend on the lower layers,our suggested structure has an advantage. For example, adding a security layer may reduce wireless redundancy but safeguard the wired portion. Partially overlapping security measures may be a trade-off concerning both ends. Even if a subsystem has partial protection, end-to-end securities are nevertheless accomplished. To be sure, some security redundancy is desirable.A secured technique for entering a network concerning authorized entrance is required in wireless segments. In making this more complicated in circumventing security steps, security professionals often use the phrase defense-in-depth (DiD).

Hence, redundancy, or defense-in-depth, offers benefits in security. Regarding end-to-end safety and security in wireless/wired networks, our suggested architecture must be clear regarding the basic media of transmission and is dependent on the "black channel."

4. Integrating Seamlessly for Secured and Safe Wireless / Wired Communication

With current automation equipment and standards, we show our proposed framework's security and safety utilizing WirelessHART, IO of Profinet and Profisafe technologies. Oursecurity modules allow us to counterfit security into the IO of Profi- Net. As our suggested structure is methodically neutral, other schemes may also be employed. In order to accomplish secure end-to-end communication, various methods (ISA100.11a, IEEE 802.15.4) can reach varying levels of integration, engineering efficiency, and performance. Providing merely gateway (GW), capabilities is inadequate for the end-users nowadays. As a replacement or complement to current technologies, new technologies and solutions are anticipated to be similar or superior. Presetting an integration approach for WirelessHART for systems automation by applying Profinet IOis employed.

4.1. Model for Communication

Data of IO was utilized in transmission procedure measures to and from gadgets, whereas Record Data is used to carrying device configuration data. Subslots may also provide diagnostic data, including process or device alarms, across the network. Modeling Profinet IO devices so requires subslots (submodules). As a container for subslots, A slot (instance of a module) is used. We model WirelessHART functionality as submodules and Physical WirelessHART devices as modules. It allows us to decouple functionality from a device, which is quite beneficial. In this way, we may represent WirelessHART functions as submodules independent of a device. Assigning capabilities (sub-Modules) to devices is represented as modules, regardless of their capabilities (module).

Deuxièmement, as shown in Figure 2, our system offers data processing, parametrization and diagnostics pertaining to every function of WirelessHART, two sub-modules of A module with models network management. In order to download the ID of the Network to a specific manager of the network, Network ID Sub-modules only provide Record information (Configuration Data). The second submodule contains the Join Key configuration data needed by the network management during the WirelessHART device joining process. The DCS can model and extend additional functionality that requires remote configuration. Using current engineering tools, we can centrally develop and disseminate configuration data to network administrators. Figure 2 shows three submodules in the second module, field device. The tag name was applied through gateways in mapping automatically Profinet IO subslot/slot destined at devices of WirelessHART, while the second submodule contains just configuration data. To resolve the addresses of WirelessHART devices, the gateway queries the tag's name.

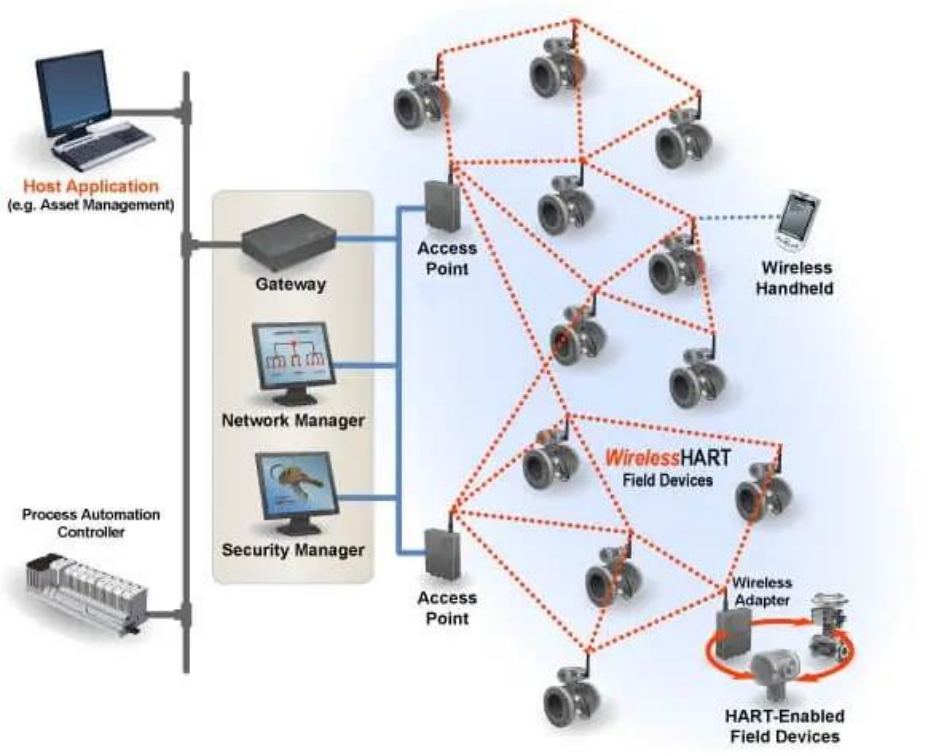

Fig. 2 WirelessHART modules and communication

Consequently, it maps them entirely in Slots by implementing the Name of the Tag contained within the subslot. Other HART Commands that DCS will transfer to WirelessHART's gadgets include burst rate, mode, and message. These models may be used to model, set up, and manage WirelessHART devices and HART commands. To develop and manage WirelessHART networks centrally, our suggested integration solution uses current engineering tools in the DCS. This reduces downtime by downloading the configuration immediately after replacing damaged components, making engineering and maintenance of WirelessHART systems easier. Moreover, the model's segregation of HART's instructions, logical and physical logical units simplifies both gateway's design and, more importantly, its use in terms of safety. Other current integration work or approaches may be employed but are unlikely to benefit safety, end-to-end security, engineering, or maintenanceoperations.

4.2. On-Demand Configuration Data

Data should only be distributed once to limit the risk of cryptographic key compromise. The cryptographic keys should be changed often to prevent key identification from the ciphertext. Our approach uses Profinet IO's Discovery and Configuration Protocol (DCP) to send keys from the station of Engineering destined for gateways of WirelessHART. Manufacturer-specific memory of non-volatile nature is present inGateway's WirelessHART program the keys.

This information is sent to WirelessHART devices via the WirelessHART Gateway in the ciphertext. Enabling this feature inthe Profinet IO standard does not need any changes to the way cryptographic keys are allocated. Modules de sécurité Using the same principle [28], Profinet IO and WirelessHART may share keys easily. Sensitive data should be transferred with more security than IP addresses. In order to apply additional security measures such as encryption, revisions must be made to the Profinet IO standard. This technique replaces the manual procedure with a regular automatic service to facilitate automated key updates. In order to connect with the network and build the key update's secured channel, WirelessHART Device must first be set up through a local port. Key distribution is a common and well-known automated issue, even in this scenario. In the absence of a formal standard for key distribution, ourtechnique should be considered an interim solution. No matter how it is implemented, our solution fills a critical need in field automation equipment security.

4.3. Communication with Security Modules

Deploying a defense-in-depth approach for industrial field networks is also crucial. Profinet IO Security Modules [29] enable the addition of a security layer without altering the underlying transmission mechanism or standards. End-to-end network security is provided by employing security modules at the highest level of Profinet IO. Added to the current modules are security modules in the GSD file.

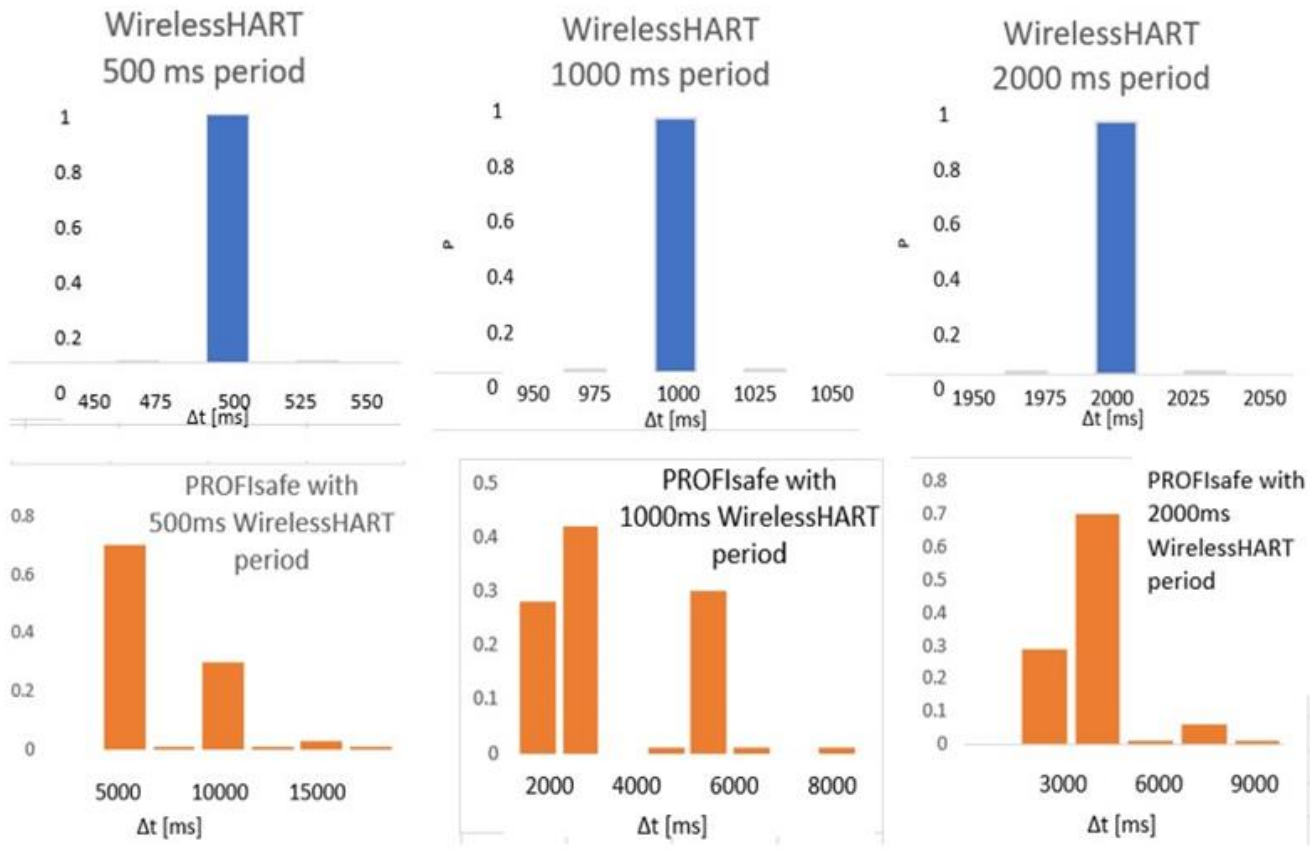

Fig. 3 Distributions of WirelessHART telegrams [upper] and theprofisafe toggle-bits [lower] w. r. to their time sequences

These standard modules or security modules may get initiated and cohabit based on actual securities risk assessment. Securing I/O information in Profinet IO is done through security modules. Section 4-2 describes how cryptographic keys for security modules are delivered. Thus, security modules work well with WirelessHART Integration utilizing Profinet IO. Cabled and cable-less fieldbus intercommunication is secured utilizing the black channel concept by integrating Modules of security Modules having suggested Wireless HART assembling.

4.4. Response time of Safety Function

Momentum is a significant key indicator concerning critical safety uses as defined by Profisafe, the time of worst-case scenarios until a state of safety is obtained when the safety function fails [29]. SFRT needs vary from millisecond to second based on various uses. In accordance with IEC 61784-3-3, our Approach' to SFRT is as follows. To calculate the overall safety function delay, sum the sensor DCS (F Host), (F Device), bus, and actuator (F Device) delays. There is a worst-case delay time and best-case for each entity I, denoted by WCDTi. Watchdog timer WDTimei is present in every entity for safety purposes, asin Eq. (1). One Fault Delay Time is specified as OFDT, and TcyF Host is the DCS period time. When a new VCN is identified, the Device Acknowledgment Time (DAT) is needed in computing a novel PDU safety as in Eq. (2). A watchdog timeout is defined as [30] for Profisafe as in Eq. (3).

$$F_{WD_{Time}} = 2T_{CY} + DAT + HAT \quad (1)$$

$$F_{WD_{Time}} = 2T_{CY_{PNIO}} + 2T_{CY_{WH}} + DAT + HAT + WCDT_{GW} \quad (2)$$

$$SFRT = \sum_{i=1}^{n} WCDT_i + \max_{i=1,2,\dots n} (WDDime_i - WCDT_i) \quad (3)$$

5. Implementation and Performance Evaluation

Automation system 800xA communicates with WirelessHART gateway through Profinet IO in proof-of-concept implementation. WirelessHART network has one device. In order to discover bottlenecks and limiting factors, the test setup is basic. The performance assessment scenario may be changed to a more realistic setting whenever appropriate. We measured the overall attainable safety function reaction time by varying the WirelessHART device's burst rate Tcy_{WH} as in Eq. (4). Being a dark channel, and security is not clearly evaluated. This paper does not discuss the security assessment of the cryptographic techniques utilized.

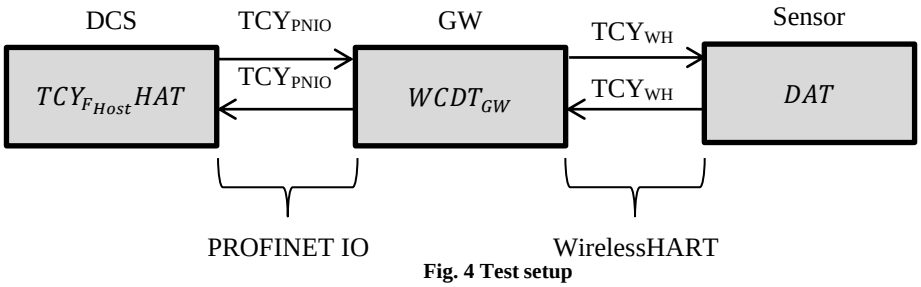

Fig. 4 Test setup

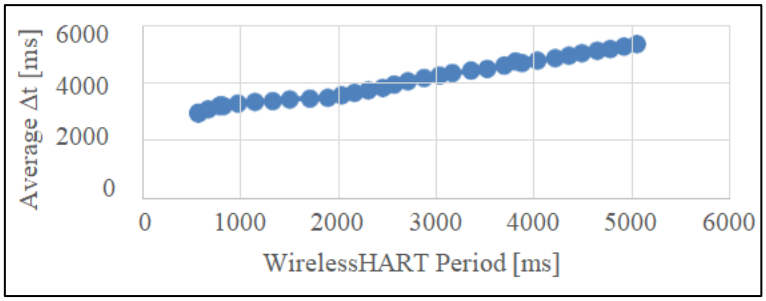

Fig. 5 Average time between transitions

There is an additional MIC that is sent together with the safety-critical data to ensure packet authenticity and integrity. This MIC has no impact on overall runtime performance.

$$Tc_{WH} = \{500,1000,2000,3000,4000,5000\}[ms] \quad (4)$$

Figure 3 depicts the frequency distribution of the periods. To plot the time interval amongst 2 consecutive WirelessHART telegrams. A similar frequency distribution is presented in the bottom plots. By synchronizing the Profisafe state machines, the toggle bit indirectly detects protocol timeouts [31]. On the other hand, upstream data is delivered on a periodic basis. TcyWH >3000 ms, probabilities were dispersed as multiplicative factors about TcyWH when tProfisafe was analyzed. The correspond- ing test setup is shown in the Figure 4.

For TcyWH and tProfisafe, the average duration between transitions is shown in Figure 5. TcyWH does not correlate to tProfisafe. Because WirelessHART fails to offer timely facilities to devices from the gateway. Additionally, unsynchronized processes in nodes and network components cause delays. As the transmission of downlink was a better effort, delays are not obvious on the graph until TcyWH is 5 seconds. This is an order of magnitude faster than network component delays sent from the device to the network management; periodic telegrams take 500-5.6 ms, assuming TcyWH =500 ms. Here, 14.5 seconds serve as a long time in the Automation arena (SFRT is normally in the seconds to milliseconds range based on the need for application safety).

Additional wireless network nodes can greatly raise SFRT as a point that only some applications will profit from functions of wireless safety by applying present protocols, e.g. notably, the proposed technique achieves the safety integrity level. A concrete TcyW H by not disturbing along WirelessHART's automatic-healing attributes will be studied instead of more comprehensive performance measurements. Due to the black channel approach, we may improve TcyWH and shorten the minimum SFRT without compromising safety.

6. Conclusion

Wired fieldbuses are now being supplemented by wireless devices and cable-less frameworks. Utilizing infrastructure wirelessly in automation necessitates resolutions having identical features compared to wired infrastructures. In today's world, there exists not a single resolution which includes operational safety for wireless; in the context of industrial automation, cable fieldbuses lack security enhancements. Such features' absence may pose serious issues while combining the latest wireless/wired gadgets in current automation systems. With this research, an integrated architecture of wireless sensor networks was offered by us. Safety and security measures may coexist with our proposal, depending on the existing requirements. Integrity and authentication mechanisms for existing automation systems may be adapted using security modules. With the system of industry Automation combining Profinet IO, WirelessHART and Profisafe, we show the proposed architecture. Predictable and timely downlinks broadcast to gadgets of WirelessHART from WirelessHART's gateways were required, according to our tests. To solve this issue, we added deterministic and periodic downlink communications addressed to WirelessHART. WirelessHART actuators that need periodic and predictable set-point transfers may be used successfully.

References

[1] Johan Åkerberg et al., "Efficient Integration of Secure and Safety Critical Industrial Wirelesssensor Networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 100, 2011. [CrossRef] [Google Scholar] [Publisher link]

[2] Tao Zheng, Mikael Gidlund, and Johan ÅkerbergWirArb, "A New MAC Protocol for Time Critical Industrial Wirelesssensor Network Applications," *IEEE Sensors Journal*, vol. 16, no. 7, pp. 2127-2139, 2015. [CrossRef] [Google Scholar] [Publisher link]

[3] Alessandra Flammini, "Wired and Wireless Sensor Networks for Industrial Applications," *Microelectronics Journal*, vol. 40, no. 9, pp. 1322-1336, 2009. [CrossRef] [Google Scholar] [Publisher link]

[4] Tifenn Rault, Abdelmadjid Bouabdallah, and Yacine Challal, "Energy Efficiency in Wireless Sensor Networks: A Top-down Survey," *Computer Networks*, vol. 67, pp. 104-122, 2014. [CrossRef] [Google Scholar] [Publisher link]

[5] Vehbi C. Gungor, and Gerhard P. Hancke, "Industrial Wireless Sensor Networks: Challenges, Design Principles, and Technical Approaches," *IEEE Transactions on Industrial Electronics*, vol. 56, no. 10, pp. 4258-4265, 2009. [CrossRef] [Google Scholar] [Publisher link]

[6] Hamad Ali H. Alawad, and Sakdirat Kaewunruen, "Wireless Sensor Networks," 2004.

[7] Bharat Bhushan, and Gadadhar Sahoo, "Requirements, Protocols, and Security Challenges in Wireless Sensor Networks: An Industrial Perspective," *Handbook of Computer Networks and Cyber Security*, Springer, Cham, pp. 683-713, 2020. [CrossRef] [Google Scholar] [Publisher link]

[8] Johan Åkerberg, Mikael Gidlund, and Mats Björkman, "Future Research Challenges in Wireless Sensor and Actuator Networks Targeting Industrial Automation," *9th IEEE International Conference on Industrial Informatics*, 2011. [CrossRef] [Google Scholar] [Publisher link]

[9] M. Supriya, and T. Adilakshmi, "Secure Routing using ISMO for Wireless Sensor Networks," *SSRG International Journal of Computer Science and Engineering*, vol. 8, no. 12, pp. 14-20, 2021. [CrossRef] [Publisher link]

[10] Mohammed Y. Aalsalem et al., "Wireless Sensor Networks in Oil and Gas Industry: Recent Advances, Taxonomy, Requirements, and Open Challenges," *Journal of Network and Computer Applications*, vol. 113, pp. 87-97, 2018. [CrossRef] [Google Scholar] [Publisher link]

[11] V. Çagrı Gungör, and Gerhard P. Hancke, *Industrial Wireless Sensor Networks: Applications, Protocols, and Standards*, CRC Press, 2013. [Google Scholar] [Publisher link]

[12] Kamrul Islam, Weiming Shen, and Xianbin Wang, "Wireless Sensor Network Reliability and Security in Factory Automation: A survey," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 42, no. 6, pp. 1243-1256, 2012. [CrossRef] [Google Scholar] [Publisher link]

[13] Mohsin Raza et al., "A Critical Analysis of Research Potential, Challenges, and Future Directives in Industrial Wireless Sensor Networks," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 39-95, 2018. [CrossRef] [Google Scholar] [Publisher link]

[14] B. Anjanee Kumar, N. Anuradha, and M. Supriya, "Routing and Securing the Clustered Step Sized Wireless Sensor Networks," *SSRG International Journal of Mobile Computing and Application*, vol. 4, no. 1, pp. 13-20, 2017. [CrossRef] [Publisher link]

[15] Petcharat Suriyachai, Utz Roedig, and Andrew Scott, "A survey of MAC Protocols for Mission-critical Applications in Wireless Sensor Networks," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 2, pp. 240-264, 2012. [CrossRef] [Google Scholar] [Publisher link]

[16] Juan Aponte-Luis et al., "An Efficient Wireless Sensor Network for Industrial Monitoring and Control," *Sensors*, vol. 18, no. 1, p. 182, 2018. [CrossRef] [Google Scholar] [Publisher link]

[17] Kay Soon Low, Win Nu Nu Win, and Meng Joo Er, "Wireless Sensor Networks for Industrial Environments," *International Conference on Computational Intelligence for Modelling, Controland Automation and International Conference on Intelligent Agents, Web Technologies and Internet Commerce (CIMCA-IAWTIC'06)*, 2005. [CrossRef] [Google Scholar] [Publisher link]

[18] H.S. Ng, M.L. Sim, and C.M. Tan, "Security Issues of Wireless Sensor Networks in Healthcare Applications," *BT Technology Journal*, vol. 24, pp. 138-144, 2006. [CrossRef] [Google Scholar] [Publisher link]

[19] R. Manoj Kumar, and S. Sridevi, "A Survey on Localization Methods in Wireless Sensor Networks," *SSRG International Journal of Computer Science and Engineering*, vol. 4, no. 4, pp. 13-17, 2017. [CrossRef] [Publisher link]

[20] Matteo Baire et al., "A wireless Sensors Network for Monitoring the Carasau Bread Manufacturing Process," *Electronics*, vol. 8, no. 12, p. 1541, 2019. [CrossRef] [Google Scholar] [Publisher link]

[21] Vehbi Cagri Gungor, "Industrial Wireless Sensor Networks," *Industrial Communication Systems*, 2016.

[22] Ivanovitch Silva et al., "Reliability and Availability Evaluation of Wireless Sensor Networks for Industrial Applications," *Sensors*, vol. 12, no. 1, pp. 806-838, 2012. [CrossRef] [Google Scholar] [Publisher link]

[23] Pooja, Manisha, and Yudhvir Singh, "Security Issues and Sybil Attack in Wireless Sensor Networks," *International Journal of P2P Network Trends and Technology*, vol. 3, no. 1, pp. 1-6, 2013. [Google Scholar] [Publisher link]

[24] Marko Paavola, and Kauko Leiviska, "Wireless Sensor Networks in Industrial Automation," *Intech Open*, 2010. [CrossRef] [Google Scholar] [Publisher link]

[25] Francesco Flammini et al., "Towards Wireless Sensor Networks for Railway Infrastructure Monitoring," *Electrical Systems for Aircraft, Railway and Ship Propulsion*, 2010. [CrossRef] [Google Scholar] [Publisher link]

[26] Md. Motaharul Islam et al., "A Survey on Virtualization of Wireless Sensor Networks," *Sensors*, vol. 12, no. 2, pp. 2175-2207, 2012. [CrossRef] [Google Scholar] [Publisher link]

[27] Priyanka Rawat et al., "Wireless Sensor Networks: A Survey on Recent Developments and Potential Synergies," *The Journal of Supercomputing*, vol. 68, pp. 1-48, 2014. [CrossRef] [Google Scholar] [Publisher link]

[28] Carlos F. García-Hernández et al., "Wireless Sensor Networks and Applications: A Survey," *IJCSNS International Journal of Computer Science and Network Security*, vol. 7, no. 3, pp. 264-273, 2007. [Google Scholar]

[29] Jia Zhu, Yulong Zou, and Baoyu Zheng, "Physical-Layer Security and Reliability Challenges for Industrial Wireless Sensor Networks," *IEEE Access*, vol. 5, pp. 5313-5320, 2017. [CrossRef] [Google Scholar] [Publisher link]

[30] Wootae Jeong, and Shimon Y. Nof, "Performance Evaluation of Wireless Sensor Network Protocols for Industrial Applications," *Journal of Intelligent Manufacturing*, vol. 19, pp. 335-345, 2008. [CrossRef] [Google Scholar] [Publisher link]

[31] Wiem Elghazel et al., "Dependability of Wireless Sensor Networks for Industrial Prognostics and Health Management," *Computers in Industry*, vol. 68, pp. 1-15, 2015. [CrossRef] [Google Scholar] [Publisher link]